IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Farmer et al.	Patent Application	
Serial No.:	10/669,784	Group Art Unit:	2186
Filed:	September 24, 2003	Examiner:	Tsai, Sheng Jen

For: System and Method to Protect Vital Memory Space From Non-Malicious Writes In a Multi Domain System

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1, 3-5, 8-13, 15, 16, 19 and 20 remain pending. Claims 1, 3-5, 8-13, 15, 16, 19 and 20 stand rejected. Rejections of Claims 1, 3-5, 8-13, 15, 16, 19 and 20 are herein appealed.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites a method (200 of Figure 2 and page) for protecting memory space in a target storage device during a write operation in a computer system. The method includes creating (400 of Figure 4 and page 5, paragraph 23) a single data packet, including user data that is to be written in a write operation to said target storage device and key data that is used to establish authorization to store said user data, said key data being generated based upon a destination address of said write operation and based on a portion of said user data, transmitting (202 of Figure 2 and page 5, paragraph 24) said single data packet to the target storage device, determining (203 of Figure 2 and page 6, paragraph 24) whether said key data is valid and writing (204 of Figure 2 and page 6, paragraph 24) said user data into said target storage device only when said key data is valid.

Independent Claim 8 recites a system (300 of Figure 3 and page 5, paragraph 22) for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising means (301 of Figure 3 and page 5, paragraph 22) for simultaneously delivering user data and key data to a controller (302 of Figure 3 and page 5, paragraph 22) of said storage device in a single data packet , wherein said user data is to be written to said storage device and said key data is used to establish authorization to store said user data, said key data being generated based upon a system clock setting of said computer system, based on a destination address of a write operation

and based on a portion of said user data and means for determining whether said key data authorizes writing said user data to said storage device (303 of Figure 3 and page 5, paragraph 22).

Independent Claim 15 recites A computer program product having a computer readable medium (504 of Figure 5 and page 7, paragraph 30) having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system (500 of Figure 5 and page 7, paragraph 30), the computer program product comprising code for composing (400 of Figure 4 and page 5, paragraph 23) a single data packet including user data and key data, wherein said user data is to be written to said target storage device in a write operation and said key data is used to establish authorization to store said user data, said key data being generated based upon a portion of said user data and a destination address of said write operation and a system clock setting of said computer system, code for transmitting (202 of Figure 2 and page 5, paragraph 24) said single data packet to said target storage device and code for determining (203 of Figure 2 and page 6, paragraph 24)whether said key data is valid.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1, 3-5, 15-16 and 19-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Garcia et al (6,151,689) in view of Taguchi et al. (5,915,025).

2. Claims 8-13, 15-16, and 19-20 stand rejected under 35 U.S.C. 103(a), as being unpatentable over Garcia et al (6,151,689) in view of Adler et al. (4,255,811) and yet in further view of Taguchi.

Arguments

1. Whether Claims 1, 3-5, 15-16 and 19-20 are patentable over Garcia et al (6,151,689) in view of Taguchi et al. (5,915,025).

Appellants have reviewed the above-cited references and respectfully submit that the embodiments as recited in Claims 1, 3-5, 15-16 and 19-20 are patentable over Garcia in view of Taguchi for at least the following rationale.

Claim 1 recites (emphasis added):

> creating a single data packet, including user data that is to be written in a write operation to said target storage device and key data that is used to establish authorization to store said user data, said key data being generated based upon a destination address of said write operation and based on a portion of said user data;

The Examiner cites Garcia as teaching a "single data packet....including user data." However, Appellants respectfully disagree and respectfully submit that Garcia and Taguchi fail to teach or suggest this claimed feature. Garcia refers to the data in the packets of Figures 3A-4C as "input/output data" and does not teach or suggest user data, as claimed.

Appellants submit that neither Garcia nor Taguchi, alone or in combination teach or suggest this claimed feature. Specifically, embodiments of the present invention enable simultaneous transmission of user data and key data in a single

packet which decreases the time period for which the target device is vulnerable to an erroneous data transmission.

However, with Taguchi, the key data is not sent in a single data packet with the user data, as claimed. Taguchi provides details for how to generate key data. However, Taguchi actually teaches away from the claimed feature of a single data packet by teaching the key and the data are sent separately. In column 7, line 60 through column 8, line 6. Taguchi teaches "The encrypted data is placed in the storage means. When a request is made by the control means to process the encrypted data, the decryption key generation means generates the decryption key. This is very different from generating the key data based on the user data and sending it in a single data packet with the user data, as claimed.

For at least the foregoing rationale, Appellants respectfully submit that Claim 1, and similarly Claims 8 and 15, are patentable over Garcia in view of Taguchi under 35 U.S.C. § 103(a). As such, allowance of Claims 1, 3-5, 15-16 and 19-20 is respectfully requested.

2. Whether Claims 8-13, 15-16, and 19-20 are patentable over Garcia et al (6,151,689) in view of Adler et al. (4,255,811) and yet in further view of Taguchi.

As stated above, Appellants submit that Garcia and Taguchi fails to teach or suggest the feature "a single data packet with user data." Appellants further submit that Adler fails to remedy the deficiencies of Garcia and Taguchi.

Specifically, Adler fails to teach or suggest a single data packet with user data, as claimed.

For at least the foregoing rationale, Appellants respectfully submit that Claim 8, and similarly Claim 15, are patentable over Garcia in view of Adler and Taguchi under 35 U.S.C. § 103(a). As such, allowance of Claims 8-13, 15-16, and 19-20 is respectfully requested.

Conclusion

In light of the above amendments and remarks, Appellants respectfully request allowance of Claims 1, 3-5, 8-13, 15, 16, 19 and 20.

The Examiner is invited to contact Appellants' undersigned representative if the Examiner believes such action would expedite resolution of the present application.

Respectfully submitted,
WAGNER BLECHER LLP

Date: 08/03/2009

/John P. Wagner, Jr./

John P. Wagner, Jr.
Reg. No. 35,398

WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
(408) 377-0500

Claims Appendix

1. A method for protecting memory space in a target storage device during a write operation in a computer system, the method comprising:

creating a single data packet, including user data that is to be written in a write operation to said target storage device and key data that is used to establish authorization to store said user data, said key data being generated based upon a destination address of said write operation and based on a portion of said user data;

transmitting said single data packet to the target storage device;

determining whether said key data is valid; and

writing said user data into said target storage device only when said key data is valid.

3. The method of claim 1 further comprising:

performing a boolean operation on selected bits of said user data to generate said key data.

4. The method of claim 1 further comprising:

generating verification data from said user data at a controller of said target storage device; and

comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data.

5. The method of claim 4 further comprising:

storing said user data to said target storage device if said key data matches said verification data.

8. A system for conducting a protected memory write to a storage device in a single transaction within a computer system, the system comprising:

means for simultaneously delivering user data and key data to a controller of said storage device in a single data packet , wherein said user data is to be written to said storage device and said key data is used to establish authorization to store said user data, said key data being generated based upon a system clock setting of said computer system, based on a destination address of a write operation and based on a portion of said user data; and

means for determining whether said key data authorizes writing said user data to said storage device.

9. The system of claim 8 further comprising:

means for writing said user data to said storage device only when said key data authorizes writing said user data.

10. The system of claim 8 further comprising:

means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device.

11. The system of claim 10 wherein said algorithm calculates said key data from said user data.

12. The system of claim 8 wherein said determining means further comprises:

means for generating verification data at said storage device controller; and

means for comparing said verification data to said key data.

13. The system of claim 8 wherein said determining means further comprises:

means for authorizing writing of said user data only where said verification data matches said key data.

15. A computer program product having a computer readable medium having computer program logic recorded thereon for protecting memory space in a target storage device during a write operation in a computer system, the computer program product comprising:

code for composing a single data packet including user data and key data, wherein said user data is to be written to said target storage device in a write operation and said key data is used to establish authorization to store said user data, said key data being generated based upon a portion of said user data and a destination address of said write operation and a system clock setting of said computer system;

code for transmitting said single data packet to said target storage device; and

code for determining whether said key data is valid.

16. The computer program product of claim 15 further comprising:

code for writing said user data into said target storage device only when said key data is valid.

19. The computer program product of claim16_wherein the code for determining comprises:

code for generating verification key data from said user data at a controller of said target storage device; and

code for establishing said calculated key data as valid only if said generated verification key data matches said key data included in said single data packet.

20. The computer program product of claim 19 wherein said the code for generating verification data comprises:

code for repeating said step of calculating key data at said controller of said target storage device.

Evidence Appendix

None

Related Proceedings Appendix

None